

VU Research Portal

Clickfraude, waan of werkelijkheid

van den Hoven van Genderen, R.; Lodder, A.R.

published in

Tijdschrift voor Internetrecht
2008

document version

Peer reviewed version

[Link to publication in VU Research Portal](#)

citation for published version (APA)

van den Hoven van Genderen, R., & Lodder, A. R. (2008). Clickfraude, waan of werkelijkheid. *Tijdschrift voor Internetrecht*, (5), 114-118.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

E-mail address:

vuresearchportal.ub@vu.nl

This is a postprint of

Clickfraude, waan of werkelijkheid

Hoven van Genderen, R. van den, Lodder, A.R.

Tijdschrift voor Internetrecht(5), 114-118

Published version: no link available

Link VU-DARE: <http://hdl.handle.net/1871/47604>

(Article begins on next page)

Clickfraude, waan of werkelijkheid?

Rob van den Hoven van Genderen & Arno R. Lodder¹

Na jarenlange strijd en animositeit werd in oktober 2008 bekend dat Google en Click Forensics voortaan gingen samenwerken. Google haalt vrijwel al haar inkomsten uit reclame-uitingen. Hoewel er verschillende varianten bestaan van de zogenaamde Pay per click ads maakt de naam het financieringsmodel dat eraan ten grondslag ligt helder: iedere click levert in beginsel geld op voor Google. Click forensics is marktleider in het opsporen van abusievelijke of frauduleuze clicks. Hun doel is te voorkomen dat de plaatser van de reclame onnodig veel betaalt. In dit artikel wordt achtereenvolgens ingegaan op het fenomeen “click industrie”, click fraude, de juridische duiding van dit verschijnsel en de praktische inleiding

Internet is een niet weg te denken inkomstenbron voor miljoenen ondernemers. Naast directe koop- en verkoop van diensten en producten, wordt veel geld verdiend aan aandachttrekkers die uiteindelijk moeten resulteren in verkoop van deze producten of diensten: banners, gesponsorde links, korte filmpjes, etc. Voor deze reclame-uitingen kan op verschillende manieren betaald worden. Zo kan net als bij een advertentie in de krant, door de adverteerder betaald worden voor het plaatsen van de link of banner of voor een bepaalde periode zoals bij reclame bij bushokjes of langs de snelweg. Net als bij radio en tv kunnen kijkcijfers (aantal bezoekers van een site) invloed hebben op de bedragen die voor de reclame betaald moet worden.

Het internet biedt naast al deze bestaande financieringsmogelijkheden ook een zeer nauwkeurig financieringsmodel. Bijzonder hieraan is dat niet betaald wordt voor het kijken naar de reclame. Pas op het moment dat internetgebruikers na het zien van de commerciële informatie besluiten op de link of banner te clicken, dan levert deze click voor de verkoper van de reclame (bijvoorbeeld Google) een bedrag tussen enkele centen en enkele euro's op. De gedachte hierachter is dat als bezoekers op een advertentie of ander klikwaardig item klikken, zij het geadverteerde product overwegen te kopen. Wat nu als blijkt dat er op een website plotseling enorm veel op een advertentie geklikt wordt, zonder dat dit tot maar één verkoop leidt? Is dit toeval of is er iets anders aan de hand als er sprake is van ‘klikken, klikken, niet kopen’?

Bedrijven als Clickfraud.com en Doogleonduty.com leggen zich toe op het voorkomen van misbruik van *Pay Per Click Ads*, waarvan de bekendste Google Adwords is. Dit zijn advertenties waarbij de adverteerder betaalt voor iedere internetgebruiker die op de advertentie clickt. In 2006 waren grootschalige misbruikzaken in het nieuws, Google en Yahoo troffen schikkingen voor tientallen miljoenen euro's.² Hoewel het sinds die tijd relatief rustig is gebleven, is ook in de zomer van 2008 in Amerika een class action zaak gestart omtrent vermeend misbruik.³

Google is marktleider en heeft hierdoor deze vorm van adverteren en tevens de service naar haar adverteerders gedefinieerd. In de “pay-per-click” advertentiemarkt ging in 2006 10

¹ Rob van den Hoven van Genderen is verbonden aan het Computer/Law Institute van de Faculteit rechtsgeleerdheid van de VU, juridisch consultant en onder andere als adviseur werkzaam bij SwitchLegal advocaten. Arno Lodder is eveneens verbonden aan het Computer/Law Institute.

² Referentie

³ Referentie

miljard euro om,⁴ een bedrag dat waarschijnlijk alleen maar is toegenomen. Deze geldstroom loopt met name via de grote zoekmachines Google, Yahoo en AOL.com.

In deze bijdrage wordt ingegaan op de clickindustrie en clickfraude en worden de juridische aspecten ervan belicht.

1 - De “clickindustrie”

De grote start- of openingssites als Yahoo en Google, maar ook veilingssites (eBay, Marktplaats) en de meeste commerciële sites geven de mogelijkheid om reclamelinks te plaatsen. Via tekst, icoon of banner kan worden doorgeklikt naar de site van de partij die zijn diensten of producten aanbiedt. Verder kan het klikken op keywords verbinding met daaraan gerelateerde sites genereren. De ook uit de Nederlandse jurisprudentie bekende Google Adwords⁵ worden gebruikt om door de adverteerder opgegeven keywords te koppelen aan de reclame-uiting. De aanbieder van tweedehands auto's kan bijvoorbeeld als keyword Volvo, occasion, etc. opgeven. Google doet op verzoek ook suggesties over wat goede zoekwoorden zijn om de reclameboodschap aan te koppelen. Een bij Google gekochte reclamelink verschijnt behalve op de site van Google ook op allerlei andere sites, waaronder ook sites met domeinnamen met een typo of anderszins aantrekkelijke namen die nog niet in gebruik zijn en alleen voor reclame worden gebruikt.

Wie zijn site bovenaan wil zien in lijstjes bij de zoekmachines, of op startsites het eerste naar voren wil komen, maakt hiervoor gebruik van dienstverleners als Google. Tussen de dienstverlenende zoekmachine of “hostsite” en de adverterende partij worden afspraken gemaakt over classificatie van trefwoorden en/of plaatsing van banners of andere clickwaardige items als iconen of teksten. Hierbij wordt bepaald voor welke trefwoorden de betreffende partij bovenaan komt bij zoekopdrachten, waarna wordt aangegeven hoeveel wordt betaald voor elke bezoeker die via deze weg op de site binnenkomt. Hoe hoger men komt of hoe eerder men aangeklikt wordt, hoe hoger het tarief, hetgeen natuurlijk ook afhankelijk is van de populariteit van de gastheersite.

De tarieven variëren van een paar eurodubbeltjes tot enkele euro's per click. Daarnaast bieden Yahoo en Google ook contextual advertising als Content Match en AdSense. Bij ‘contextual advertising’ worden advertenties getoond op deelnemende webpagina's die er contextueel bij passen. Het aanbod van links kan daardoor op een erg persoonlijke wijze worden samengesteld. Als je in Google een mailtje schrijft over juridische aspecten van sociale netwerksites, zullen er allemaal links van dergelijke aanbieders verschijnen. Ook kan, zoals bij LinkedIn, een mannelijke gebruiker links te zien krijgen die doorverwijzen naar sites waar dames op zoek zijn naar een relatie met heren en omgekeerd. Dit zijn betrekkelijk onschuldige voorbeelden, maar door de aanbieders van de links worden bij gelegenheid ongetwijfeld gevoelige gegevens in de zin van de Wbp verwerkt. Wanneer de bezoeker op zo'n contextuele advertentie klikt, krijgt de partner of de eigenaar van de site waarop de advertentie werd getoond een gedeelte van het bedrag dat de adverteerder voor de click moet betalen. Clickomzet (en fraude) ontstaat onder andere doordat zoekmachines de advertenties die ze verkopen ook op andere websites laten plaatsen. Deze websites delen mee in de omzet, wat sommigen ertoe verleidt software aan het werk te zetten die de advertenties aanklikt.

⁴ Zie ter illustratie artikel Wired magazine 14.01 2006. <http://www.wired.com/wired/archive/14.01/fraud.html>

⁵ Zie bijvoorbeeld Hof Amsterdam 14 december 2006, LJN AZ6457 en Hoge Raad 12 september 2008, LJN BF0518.

2 - Wat is clickfraude?

Omdat bij iedere bezoeker van een website kan worden vastgesteld waar deze vandaan komt, kan gekeken worden naar de zogenaamde “Click-omzet”-ratio. Stel dat je 1 euro per click betaalt en 10% van de clickers uiteindelijk iets kopen voor gemiddeld 25 euro. Dan weet je dus dat je 10 euro kwijt bent, voor 25 euro aan inkomsten. Een in dit licht voor de inkoper van links interessante functionaliteit is Googleanalytics. Hierdoor kan inzicht worden verkregen in welke trefwoorden tot de meeste omzet leiden.

De naam click(fraude) verwijst naar het geluid en handeling, de “click” met de muis die (repetitief) wordt uitgevoerd (en gehoord) door op een woord, afbeelding of icoon of gehele advertentie te klikken. Er bestaan in grote lijnen twee soorten clickfraude:

- clickfraude met het oogmerk van onrechtmatige bevoordeling van enige partij, niet zijnde de adverteerder, ook wel netwerk clickfraude genoemd;
- clickfraude met het oogmerk van onrechtmatige benadeling van de adverteerder door de concurrentie, ook wel concurrentie clickfraude genoemd.

We spreken van clickfraude door het netwerk wanneer een zoekmachine, personen of een partner (contextual advertising) manueel of softwarematig advertenties gaat aanklikken met het oogmerk de inkomsten voor derden te verhogen ten koste van de adverteerder. Dit betreft zowel een kwantitatief als kwalitatief aspect. Het aantal clicks wordt kunstmatig en opzettelijk verhoogd en daarmee de kosten voor de adverteerder vergroot. Mede als gevolg daarvan wordt de effectiviteit van de clicks bijzonder laag en leiden veel minder clicks tot aanschaf van het product of de dienst. Dit laatste is alleen in het voordeel van de zoekmachine of de aangeklikte gastheer (partner)site. Als er een sterke groei in contactmomenten met de site ontstaat zonder dat er een groei is in daadwerkelijk relevant bezoek van de site, zeker als die clicks afkomstig zijn van een relatief klein aantal IP-adressen, dan is dit een sterke aanwijzing dat er sprake is van clickfraude.

Overigens kan er ook sprake zijn van clickfraude zonder direct geldelijk voordeel. Het is niet onvoorstelbaar dat ten behoeve van het Social Science Research Network Citation Index⁶ het aantal clicks ten gunste van een bepaalde wetenschappelijke auteur kunstmatig wordt opgevoerd door bekenden of door hem zelf om zijn wetenschappelijke glans te verhogen. SSRN waarschuwt dat dergelijk misbruik wordt bestraft.

Het bewijs van clickfraude is vaak moeilijk te leveren, maar partijen nemen de aantijgingen serieus.⁷ Op 28 juni 2006 ging Yahoo akkoord met een “settlement” voor ruim 6 miljoen dollar voor het betalen van schade aan benadeelden voor clickfraude. Google heeft als gevolg van (vermeende) clickfraude in een zogenaamde “class action” in 2006 90 miljoen dollar aan de benadeelden betaald en talrijke maatregelen genomen om clickfraude te voorkomen. Sindsdien is het betrekkelijk rustig op de “clickfraude-markt”.

Volgens *Business Week* verdween een eveneens aan Google gerelateerde “duidelijke clickfraude” zaak in de doofpot om het vertrouwen in deze levensader van Google (Google-adds) niet te verstoren.⁸ Google probeert het belang van clickfraude te ontzenuwen, het is

⁶ <http://ssrn.com>

⁷ (Checkmate Strategic Group, Inc. v. Yahoo, Inc., No. 2:05-CV-04588-CAS-FMO: C.D. Cal. [preliminary settlement approved June 28, 2006](#)).

⁸ http://www.businessweek.com/technology/content/dec2006/tc20061204_923336.htm

immers slecht voor de business als dit fenomeen te veel aandacht zou krijgen. Sommige bronnen stellen dat 35 % van alle clicks “vals” zijn, ander bronnen stellen dat 5-15% meer in de buurt van de werkelijkheid komt. Het aandeel frauduleuze clicks is volgens de Amerikaanse belangenorganisatie Click Forensics in 2007 met ruim 16 % toegenomen.⁹ Het bewijs voor de juistheid van deze percentages is moeilijk te leveren. De sterk uit elkaar lopende percentages van Google en Click Forensics zullen door de recente samenwerking naar verwachting elkaar naderen. Welk percentage ook juist moge zijn, op een “clickmarkt” van meer dan 10 miljard is de schadepost aanzienlijk. Het is daarom wenselijk de mogelijkheden te benutten om die schade te beperken door technische en juridische maatregelen.

Een substantieel aandeel van clickfraude zou worden begaan door de concurrentie. Zij kunnen een query invoeren in een zoekmachine en vervolgens de betalende advertenties opzettelijk aanklikken. Dit heeft als gevolg dat degene die deze advertentie heeft gelanceerd een gepeperde rekening krijgt en het budget sneller opraakt terwijl de clicks geen afname van producten of diensten genereren. Wanneer deze frauduleuze concurrent dan zelf nog eens een heel laag budget heeft ingesteld voor diezelfde query, zal hij door de uitval van zijn concurrent na een tijdje bovenaan komen met zijn advertentie, omdat het budget van de concurrentie op is. Hij kan zo goedkope advertenties verkrijgen; dus een lage cost-per-click.¹⁰

De wijze waarop clickfraude plaatsvindt varieert. In India en China zouden bedrijven geld verdienen door personeel handmatig op advertenties te laten klikken.¹¹ Bulkclicks worden doorgaans softwarematig vanuit een klein of groter aantal IP-adressen worden gegenereerd. Dit kan zelfs gebeuren via door parasietprogramma's geïnfecteerde gastcomputers (zombies) van derden die zich van geen kwaad bewust zijn. In de DollarRevenue zaak heeft de OPTA een bedrijf aangepakt dat op meer dan 60.000 computers per dag advertentiesoftware installeerde zonder de gebruikers hierover voldoende in te lichten.¹² In totaal werden op 22 miljoen computers programma's geïnstalleerd. Door deze advertentiesoftware is door het bedrijf meer dan 1 miljoen winst gemaakt in de periode van een jaar. Aan de verschillende betrokkene werd in totaal een boete van 1 miljoen euro opgelegd. Het op 13 december 2007 ingediende bezwaarschrift is op 18 juni 2008 door de OPTA ongegrond verklaard.¹³

Daarnaast kunnen er clickgerelateerde fraudehandelingen worden verricht als eenvoudig indienen van te hoge clickrekeningen of indienen van valse rapporten. Dit kan onzes inziens echter onder “gewoon” frauduleus gedrag worden geschaard.

Oneigenlijk klikgedrag bij de gebruiker is verwant aan clickfraude. Gebruikers die wat ongeduldig met losse vingers de toetsen bespelen kunnen niet bedoelde dubbele of driedubbele clicks veroorzaken. Vaak zal deze vorm echter worden ondervangen door een technisch filter dat slechts eenmaal de click registreert. Dit aspect onder fraude te scharen lijkt wat ver te gaan. Het is de vraag of, indien er technische mogelijkheden zijn dit onderscheid te maken en deze maatregelen niet door de aanbieder/gastheersite worden gebruikt, er dan niet sprake is van onrechtmatig gedrag of nalatigheid door die partij. De Nederlandse rechter deed hierover recent een opmerkelijke uitspraak in de zaak Afab tegen Fx.nl.¹⁴

⁹ <http://www.techcrunch.com/2008/02/22/click-fraud-keeps-rising-up-15-percent-in-2007/>

¹⁰ Ter illustratie artikel Wired magazine 14.01 2006: <http://www.wired.com/wired/archive/14.01/fraud.html>

¹¹ 'India's secret army of online ad 'clickers', *Times of India* 3 May 2004.

¹² Besluit OPTA van 5 november 2007.

¹³ Besluit OPTA van 18 juni 2008 (beslissing op bezwaar DollarRevenue).

¹⁴ Rechtbank Amsterdam 12 maart 2008, LJN BF0813.

Afab betaalde 2 euro voor iedere click vanaf de site van Fx.nl. Als er vervolgens een gerichte offerteaanvraag wordt gedaan betaald Afab nog eens € 11,25. Over de iets meer dan duizend offerteaanvragen is men het eens. Het geschil handelt over het aantal in rekening gebrachte clicks. Afab heeft na eigen onderzoek en gebruik van een ontdebberingsprogramma vastgesteld dat de 8.741 clicks te herleiden zijn tot 2.594 unieke bezoekers. In het contract stond dat voor *iedere* klik moest worden betaald.

“De rechtbank is van oordeel dat de tekst van deze laatstgenoemde bepaling, mede gezien in het licht van de overige bepalingen van de overeenkomst, niet anders kan worden begrepen dan dat FX.nl Afab iedere klik vanaf haar website naar die van Afab in rekening kan brengen.”

Dit is een wat strenge uitleg van de bepaling. De uitspraak gaat overigens enkel in op het klikken vanaf het zelfde IP-adres, niet over het tijdsinterval tussen de clicks. Er mag echter van worden uitgegaan dat ontdebberingssoftware juist naar die tijdsinterval kijkt. Zeker als bedacht wordt dat Fx.nl aangeeft abusievelijke clicks, die zoals hier boven staan niet onder clickfraude vallen, gewoon in rekening te brengen:

“Afab heeft zich op het standpunt gesteld dat is overeengekomen dat, zoals zij het definieert, dubbelkliks bij facturering buiten beschouwing worden gelaten. FX.nl heeft zich op het standpunt gesteld dat op grond van de overeenkomst alleen klikfraude, het doelbewust laten oplopen van het aantal clicks, niet in rekening wordt gebracht.”

De overeenkomst wordt door de rechter dus in het nadeel van Afab uitgelegd. Gezien de stand der techniek (ontdebberingssoftware) en de praktijk op internet (de losse vingers) lijkt dit wat al te star. Een van de argumenten van Fx.nl kan vanwege het originele karakter niet onvermeld blijven:

“één persoon klikt voor verschillende doeleinden.”

Dus je klikt binnen fracties van seconden twee of drie keer op een link voor bijvoorbeeld verschillende cliënten. Niet volstrekt ondenkbeeldig, maar wel erg ver gezocht.

3 - Vaststellen clickfraude

Clickfraude kan opgespoord worden door te kijken naar het IP-adres van waar de klik afkomstig is, door gebruik te maken van cookies en ook door het clickpatroon te bestuderen. Indien het clickverkeer toeneemt zonder enig effect op de omzet van producten of diensten kan men vermoeden dat er sprake is van een toename van valse of lege clicks. Overigens zal wel aangetoond moeten worden dat die advertentieactiviteit in voorgaande perioden substantieel effect heeft gehad op de omzet. Dit is natuurlijk ook afhankelijk van activiteiten van de onderneming en de nadruk op “clickadvertenties”. De adverteerder, en eigenlijk ook een te goeder trouw werkende gastheersite of zoekmachineexploitant, zal indien er sprake is van een negatieve correlatie tussen de omzet en clicks, moeten aantonen dat er in een bepaalde periode sprake is van opvallende toename van clicks zonder effect op de omzet door die te vergelijken met andere perioden zodat het duidelijk wordt dat er sprake is van een negatieve tendens in de click-omzetratio.

Het vaststellen van clickfraude kan worden belemmerd door terughoudendheid van de gastheersite of zoekmachine-exploitant om gegevens te verstrekken of inzicht te geven in de beschermingstechnieken die worden gehanteerd. Het komt dan wel voor dat de exploitant van de gastheersite stelt dat hij de IP-gegevens niet kan overleggen uit overwegingen van privacybescherming. Het is de vraag of dit een terecht argument kan zijn. Het College Bescherming Persoonsgegevens is van mening dat een volledig IP-adres in een aantal gevallen als persoonsgegeven moet worden beschouwd: een voorwaarde is dat dit gegeven herleidbaar is tot de persoon, zoals in het geval van een provider die ook de rekeningen moet opmaken en daarom in bezit is van overige adresgegevens. Hierdoor vallen dit soort verwerkingen van IP-adressen over het algemeen onder de reikwijdte van de privacywetgeving. Maar de verschijningsvorm van het IP-adres is hier bepalend voor de persoonswaarde van de adressen: je zou kunnen stellen dat de herleidbaarheid tot personen en persoonsgegevens is uit te sluiten als de IP-adressen geanonimiseerd worden gebruikt ter vergelijking van verkeersoriginatie: daar waar de click vandaan komt. Blijkt dat vele clicks van eenzelfde IP-adres komen, dan is het vermoeden van fraude gerechtvaardigd. Door nader onderzoek kan dit worden vastgesteld. Daarenboven zou het belang van de adverteerder moeten worden meegenomen.

Omdat Google marktleider is op het gebied van “pay-per-click” advertenties is het interessant om te bezien welke maatregelen Google heeft genomen om clickfraude te voorkomen. In een mededeling aan de adverteerders stelt Google dat de beveiliging tegen clickfraude van groot belang is en dat er filtertechnieken¹⁵ worden toegepast. Overigens waren deze acties nog niet voldoende. Het is met name van belang de transparantie in de rapportages te verhogen. De adverteerders zullen op de hoogte moeten worden gesteld welke technieken worden gebruikt om clickfraude te detecteren. Recentelijk heeft Google aangegeven dat de clickfraude vrijwel nihil (0,02%) is, over het algemeen wordt van een hoger percentage uitgegaan.¹⁶ Het is interessant te bezien of nu Google de samenwerking met Click forensics is aangegaan het percentage clickfraude afneemt, gelijk blijft of toeneemt.

4 - Gronden voor aansprakelijkheid

Het mag van de aanbieder van gesponsorde koppelingen, zoekmachine of een gastheersite worden verwacht dat zorgvuldigheid wordt betracht door het nemen van voorzorgsmaatregelen teneinde fouten, onzorgvuldigheid of onrechtmatig gedrag te voorkomen. Het gebruik van “state of the art” beschermende technieken die in de markt voorhanden zijn kan worden gezien als een vereiste voor rechtmatigheid analoog aan de vereisten die worden gesteld in de e-commerce richtlijn, de privacyrichtlijn en artikel 13 van de Wet bescherming persoonsgegevens aangaande het hanteren van organisatorische en technische beschermingsmaatregelen.

De vraag is of het onrechtmatig en in strijd met de maatschappelijke zorgvuldigheid mag worden geacht als een partij deze maatregelen niet hanteert. In ieder geval moet bij een gesponsorde link op grond van de wettelijke informatieplichten geldend voor commerciële communicatie duidelijk zijn wie waarvoor betaald krijgt (art. 3:15e BW). Hoewel verdere wettelijke normering niet direct noodzakelijk lijkt, zou dit artikel op zich een logische plaats zijn om aanvullende normen op te nemen om eventuele onrechtmatigheid nader vorm te geven.

¹⁵ Welke technieken dit zijn, wordt in het midden gelaten.

¹⁶ Zie commentaren in : <http://searchengineland.com/070301-000001.php>:

Artikel 3:15e, lid 2

- a. Indien een aanbieder van een commerciële elektronische dienst enige wijze van doorkoppeling beschikbaar stelt zal die aanbieder alle reële in de markt gebruikelijke en beschikbare maatregelen en technieken dienen te benutten om onrechtmatig gedrag, gebruik of onrechtmatige toepassingen van die geleverde dienst tegen te gaan;
- b. De partij die de onder a van dit lid bedoelde dienst afneemt tegen wederdienst, zal in voldoende mate op de hoogte worden gebracht van de door de partij genomen maatregelen en technieken en zal transparante overzichten ontvangen op grond waarvan hij zijn wederdienst zal leveren.

Het is tamelijk vergaand om algemene wettelijke eisen te stellen voor een specifiek probleem waarvan op dit moment de omvang niet zeker is. De voorgestelde norm illustreert niettemin dat van belang is dat de aanbieder van advertentielinks de wederpartij goed dient te informeren alsmede technische maatregelen ter voorkoming van oneigenlijke of frauduleuze clicks dient te nemen.

4.1 Onrechtmatigheid

Behalve het in acht nemen van bovenstaande normatieve randvoorwaarden moet een adverteerder die de zoekmachine-exploitant of hostsite wil aanspreken op grond van wanprestatie of onrechtmatige daad aangeven waaruit de schade bestaat. Die bestaat natuurlijk in de eerste plaats uit de (te) hoge rekeningen als gevolg van toegenomen clickactiviteit. Verder kan omzet afnemen doordat er via netwerk- of concurrentiefraude wel veel verkeer wordt gegenereerd maar de effectiviteit van dat verkeer steeds slechter wordt. Zeker als er geen medewerking wordt verleend door de gastheer en partnersites kan het bovendien nog lang duren voordat men zich bewust is van de schade.

Als kan worden aangetoond dat onvoldoende maatregelen zijn genomen om de clickfraude tegen te gaan, kan evenals bij nalatigheid of onzorgvuldigheid in het overige maatschappelijk verkeer worden verondersteld dat er aansprakelijkheid kan worden gevestigd. Hierbij moet vooral gedacht worden aan onvoldoende maatregelen tot beveiliging. Een parallel kan worden getrokken met de automatiseerder die zijn cliënt onvoldoende beschermt tegen “malware” of andersoortige besmettingen van het systeem.

Niet alleen te weinig goede doorverwijzingen kunnen een probleem zijn, het kan ook te veel worden. In een door de Rechtbank Dordrecht op 6 augustus 2008 gewezen vonnis¹⁷ was sprake van het doorleiden van zoveel geïnteresseerden dat de daaruit volgende aanvragen niet verwerkt konden worden. Omdat er geen duidelijke afspraken gemaakt waren en partijen al geruime tijd samenwerkten, was de rechtbank van oordeel dat de aanleverende partij had kunnen weten dat de overschrijding van de gebruikelijke 750 doorverwijzingen per maand niet verwerkt konden worden. Deze doorverwijzingen (zogenaamde leads) bestonden uit offerteaanvragen die pas werden doorverwezen als de belangrijkste gegevens ingevuld waren. Door toevoeging van een nieuwe gastheersite werd de reguliere 750 in oktober 2007 fors overschreden (1648), maar ook voor de minder grote overschrijding in september 2007 (805) maximeerde de rechtbank de vordering op maandbasis op de gebruikelijke 750. De rechtbank overwoog als volgt:

¹⁷ Rechtbank Dordrecht 6 augustus 2008, LJN BE9981.

“Geeoordeeld wordt dat Independer onvoldoende rekening heeft gehouden met de gerechtvaardigde belangen van Optima door in de maanden september en oktober 2007 zóveel leads aan Optima door te leiden dat zij deze redelijkerwijs niet kon verwerken, terwijl zij wist, althans behoorde te beseffen dat Optima die niet kon verwerken.”

4.2 Ongerechtvaardigde verrijking

Men zou ook kunnen stellen dat de partij die te veel clicks in rekening heeft gebracht, kan worden aangesproken op grond van ongerechtvaardigde verrijking (artikel 6:212 BW), aangezien hij zich ten koste van de opdrachtgever heeft verrijkt door niet te presteren maar hier wel geld voor te ontvangen. Hij kan dan worden aangesproken tot het bedrag van die verrijking. De rechtbank Den Haag bepaalde vorig jaar¹⁸ dat onder omstandigheden niet alleen wordt betaald voor de geleverde prestatie, maar ook voor het niet leveren van een overeengekomen prestatie. In deze uitspraak ging het om een “switch” intermediaire dienst voor geleverde energie. Als aan dit aspect van de “clickovereenkomst”, het leveren van de dienst volgens de overeengekomen wijze, niet wordt voldaan, valt het fundament onder de bestaande overeenkomst weg en is onverschuldigd een financiële prestatie geleverd door de opdrachtgever.

Tevens kan een parallel worden getrokken met de door Jan Kabel aangegeven opvatting over kostenverschuiving waarmee de ontvanger wordt opgezaaid door het ontvangen van “spam”-faxberichten. Dit heeft de abonnee van een telecommunicatiedienst nooit gezien als een onderdeel van zijn dienstverlening. De kosten hiervoor zouden moeten worden verhaald op de dienstverlener.¹⁹

4.3 Strafrecht

Naast civielrechtelijke aansprakelijkheid speelt de strafrechtelijke pendant, het frauduleuze aspect, een rol. De activiteiten die onder de omschrijving van “clickfraude” vallen kunnen er immers op gericht zijn om zichzelf op onrechtmatige wijze te verrijken dan wel de andere partij te benadelen door middel van onoirbare handelingen. De delictsommschrijving van artikel 326 Sr (bedrog) vindt mogelijk toepassing bij het genereren van “clicks” op frauduleuze grondslag. Er kan dan immers sprake zijn van een oogmerk zichzelf of een ander wederrechtelijk te bevoordelen of een ander te benadelen door listige kunstgrepen.

Verder kan worden gedacht aan de toepassing van artikel 227a Sr, namelijk de opgave door de zoekmachine-exploitant of gastheersite van onware gegevens, in die zin dat, anders dan door valsheid in geschrift, opzettelijk niet naar waarheid gegevens worden verstrekt die er toe leiden dat betaald wordt voor de niet geleverde of niet bedoelde overeengekomen prestatie.

5 - Conclusie

De oplossing voor clickfraude kan in de eerste plaats worden gevonden in een voorhanden zijnde technische aanpak: het installeren van geavanceerde software om ongeldige clicks te filteren. Hierdoor reflecteert het uiteindelijk in rekening gebrachte bedrag zo goed mogelijk de kwaliteit van de geleverde dienst. Daarnaast is van groot belang dat partijen duidelijke afspraken maken over de hoeveelheid clicks, de te verwachten kwaliteit van de clicks en op welke wijze kan worden bepaald of clicks al dan niet in rekening moeten worden gebracht.

¹⁸ Rechtbank Den Haag 26 juli 2007, LJN BB3078.

¹⁹ <http://www.ivir.nl/publicaties/kabel/annotatie-abfabxs4all.html>

Hiermee kan in grote lijnen gerealiseerd worden dat adverteerders alleen betalen voor echte clicks en niet voor clicks die worden gegenereerd door concurrentie, internet robots of eventuele andere oorzaken. Tenslotte dient de aanbieder transparant te zijn ten aanzien van de genomen maatregelen en zorgvuldig te rapporteren aan de adverteerders over de gerealiseerde resultaten. Een “clickexploitant” kan op die manier ook aangeven dat door hem (technische) maatregelen zijn genomen om fraude (en fouten) tegen te gaan.

Hoewel de precieze omvang niet duidelijk is, kan het bestaan van clickfraude niet ontkend worden. In dit artikel is een aanzet gegeven tot nadere gedachtevorming over met name de juridische invalshoek, die helaas door de vooral in Common Law landen gebruikelijke praktijk om zaken ter voorkoming van precedentvorming in der minne te schikken vooralsnog minder in de rechtspraak gevonden kan worden. De Nederlandse rechter heeft echter dit jaar al meerdere keren uitspraak over clickfraude gedaan. Naar onze verwachting zullen de komende jaren nog verschillende zaken volgen, waarbij de in dit artikel aangegeven kaders toegepast alsmede nader uitgewerkt kunnen worden.